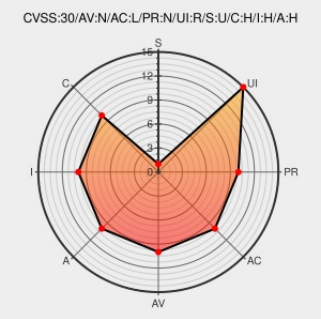
CVE-2016-1708

Published on: 07/23/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:05 PM UTC

CVE-2016-1708

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Chrome from Google contain the following vulnerability:

The Chrome Web Store inline-installation implementation in the Extensions subsystem in Google Chrome before 52.0.2743.82 does not properly consider object lifetimes during progress observation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site.

CVE-2016-1708 has been assigned by security@google.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Google Chrome Multiple Flaws Lets Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, Spoof URLs, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036428

and Execute Arbitrary Code - SecurityTracker		
[security-announce] openSUSE-SU-2016:1865-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1865
Debian -- Security Information -- DSA-3637-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3637
Google Chrome Prior to 52.0.2743.82 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 92053
[security-announce] openSUSE-SU-2016:1869-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1869
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2016/07/stable-channel-update.html
613949 - Extension install crashes browser at onDownloadProgress and onInstallStageChanged - chromium - Monorail	crbug.com text/html	CONFIRM crbug.com/613949
[security-announce] openSUSE-SU-2016:1918-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1918
[security-announce] openSUSE-SU-2016:1868-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1868
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1485
Issue 2103663002: [Extensions] Rework inline installation observation - Code Review	Issue Tracking codereview.chromium.org text/html	CONFIRM codereview.chromium.org/2103663002

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy,

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report